Office of the Legislative Auditor

State of Montana

Report to the Legislature

November 1992

EDP Audit Report

Information Processing Facility and Central Applications

Each year the Office of the Legislative Auditor audits the central computer facility and centralized computerized applications. This report provides reliance for financial-compliance and performance audits and contains recommendations for improving general controls over the mainframe computer center (Information Processing Facility) and application controls over the following systems:

- State Payroll System
- Statewide Budgeting and Accounting System
- Warrant Writing System

Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
Helena, Montana 59620

92DP-33

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration and computer science.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

Office of the Legislative Auditor

EDP Audit

Information Processing Facility and Central Applications

Members of the audit staff involved in this audit were: Jeane Carstensen, DJ Kimball, Bill Kuhl, Rich McRae, Jill Olson, and Catherine L. Scarff.

Table of Contents

Table of Contents

Department of Administration	Bob Marks, Director
	Dave Ashley, Deputy Director
	Connie Griffith, Administrator Accounting and Management Support Division
	Mike Trevor, Administrator Information Services Division
Office of the State Auditor	Andrea "Andy" Bennett, State Auditor
	Donna F. Warner, Deputy Director State Payroll Department
	Debbie Van Vliet, Administrator Fiscal Management and Control Department

Report Summary

Introduction

Our EDP Audit reviewed centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS). We performed a general control review of the state's mainframe computer and an application review of SBAS, each operated by the Department of Administration. We also performed application reviews of the State Payroll and Warrant Writer systems, operated by the State Auditor's Office. A discussion of general and application controls is included on pages 1 and 2. The objectives and scope of the audit are discussed on pages 2 and 3 of the report.

General Controls

The Department of Administration, Information Services Division (ISD), manages central data processing services for state government. Processing is performed on an IBM 3090 computer operating 24 hours a day except for times allocated for system maintenance.

In our review of ISD's general control environment, we found organizational, procedural, hardware, software, and system development controls existed and were operating as intended. However, we noted weaknesses in physical security and access controls.

Physical Security

Physical access controls ensure access to computer tapes and hardware is limited to authorized personnel. During our review of physical access controls, we determined ISD does not have a written policy for changing the computer room password. The department should document and communicate its policy for password changes to ensure adequate computer room access security is maintained. Department officials indicated they will establish a formal written policy and communicate the policy to department employees.

ISD contracts with an outside mainframe computer vendor to perform maintenance and/or repair to its computer hardware. We determined ISD personnel do not supervise maintenance personnel activities. Department officials stated the computer

vendor has employed one individual to provide mainframe maintenance to the department. They indicated logging the individual's access during regular working hours is not feasible but agreed to log access and record maintenance activities performed during other work shifts. The officials also agreed to log access full-time and record activities for all other maintenance personnel.

Access Controls

ISD uses Access Control Facility-2 (ACF2) software to provide control over electronic access to programs and data stored on the mainframe computer. We reviewed ACF2 rules written for Warrant Writer, State Payroll, and SBAS applications, and we identified access control weaknesses which are summarized below and discussed on pages 10 and 16.

Access to Production Programs and Datafiles

We determined current ACF2 rules allow Department of Administration programmers unlogged write access to some payroll and SBAS application programs. We also determined Department of Administration input/output (I/O) controllers have unlogged write access to payroll production programs and logged write access to payroll system libraries.

Write access to production programs and datafiles allows programmers to add fictitious payments and change control total balancing programs to disguise differences. Programmers do not need access to system or application libraries, which would provide a means of bypassing controls. Their activities should be restricted to test programs and files, with access only to those programs and files needed for a given assignment. I/O controller access should be logged and closely monitored.

Department of Administration and State Auditor's Office officials have agreed to closely monitor programmer access and develop alternative procedures to limit programmer access to production programs and datafiles. In addition, the State Auditor's Office has agreed to log and closely monitor I/O controller access to programs and datafiles.

Application Controls

We performed application reviews of the State Payroll, Warrant Writer, and SBAS applications. We reviewed input, processing, and output controls for each application. Overall, we concluded the controls over the applications are adequate to ensure data integrity. However, we found areas where SBAS and State Payroll application controls could be enhanced to further ensure the security and integrity of each application's data. These areas include: disaster recovery, input edit documentation, and procedure manual documentation. Additional discussion of these and other issues is included in Chapters III and IV of the report.

Disaster Recovery

We determined disaster recovery plans for SBAS and State Payroll applications should be updated and tested. The Department of Administration should include On-line Edit & Entry (OE&E) in its SBAS disaster recovery plan. The State Auditor's Office should update the payroll disaster recovery plan to include on-line payroll and on-line forms applications. Agencies use OE&E, on-line payroll, and on-line forms applications to electronically input and transfer documents to SBAS and State Payroll, respectively.

Without documented and operable disaster recovery plans, state agencies may be required to manually prepare documents and the Department of Administration or State Auditor's Office could not efficiently process the documents to ensure continued functioning of state government. The Montana Operations Manual (MOMS) section 1-0240.00 outlines agency responsibilities regarding disaster recovery. Officials of both agencies have agreed to document their disaster recovery plans.

Edit Documentation

The State Auditor's Office on-line forms application contains input edits to assist agency users when entering payroll forms. Input edits compare input data to preestablished limits and reasonableness tests. If a user enters invalid data, the edits invoke an error message requesting the user to correct the data.

We determined the office does not have a complete list of on-line forms input edits and associated error messages. State

Payroll should formally document on-line forms input edits to provide adequate support of edits and edit changes. Documented edit and error definitions provide a basis for making program modifications and facilitate testing procedures.

Procedure Manuals

The State Auditor's Office deputy director and assistant administrator procedure manuals do not provide complete explanations of duties necessary to process biweekly payroll. The positions require comprehensive knowledge of the biweekly payroll process. Procedures include but are not limited to: processing agency payroll data through validity edit programs; identifying and correcting errors; verifying completeness of data processed; and preparing payroll reports and warrants.

The current procedure manuals do not provide effective direction to backup personnel for processing biweekly payroll. Procedure manuals should be prepared which clearly define daily duties and problem resolution procedures.

Summary

In conclusion, we found the general and application controls were sufficient to ensure the integrity of data processed by the State Payroll, Warrant Writer, and SBAS applications. The weaknesses we identified could compromise the integrity of the data in the future. The Department of Administration and State Auditor's Office have acknowledged the need for improvement and have agreed to implement our recommendations.

Chapter I - Introduction

Introduction

We perform an annual electronic data processing (EDP) audit of the state's centralized data processing systems. We review centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS). We perform audit work at the Department of Administration, which maintains the state's mainframe and SBAS, and the State Auditor's Office, which operates the State Payroll system and has primary responsibility for Warrant Writer.

During our annual audit we gathered information, evaluated controls, and identified risks related to these systems. The controls we identified and tested are relied upon during financial-compliance, performance, and EDP audits for fiscal year 1991-92.

EDP Audit General and Application Controls

An EDP audit consists primarily of a review of internal controls. In an automated environment the procedures for reviewing controls are different from those used in a manual environment. However, the objective of ensuring the reliability of controls is still the same. EDP auditing may entail performing a general and an application control review. The general control review consists of an examination of the following controls and objectives:

Organizational - No one person should be able to conceal material errors or irregularities.

Procedural - Daily operations should protect against processing errors.

Hardware and Software - Hardware and systems software should identify system malfunctions and maintain operations.

System Development - System design and maintenance activities should promote system control and integrity.

Physical Controls - Loss or destruction of assets and records should be prevented and continuous operations should be assured.

Access - Access to hardware and electronic information should be limited to authorized individuals.

A general control review provides information regarding the ability to control EDP applications. Application controls are specific to a given application or a set of programs that accomplish a specific objective.

Application controls consist of an examination of the following controls and objectives:

Input - Ensure all data is properly encoded to machine form, all entered data is approved, and all approved data is entered.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals.

A review of the application documentation and audit trail is also performed. Applications must operate within the general control environment in order for reliance to be placed on them.

Audit Objectives

The objectives of this EDP audit were to determine the adequacy of:

1. General controls specific to the state mainframe computer.

2. Application controls in order to evaluate the adequacy and accuracy of data processed by the SBAS, State Payroll, and Warrant Writer applications.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We compared existing general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), General Accounting Office (GAO), and the EDP industry.

We reviewed Department of Administration's general controls related to the state mainframe environment. We interviewed department personnel to gain an understanding of the hardware

and software environment at the Department of Administration. We also examined documentation to supplement and confirm information obtained through interviews.

We examined procedures within the mainframe environment which ensure computer processing activities are controlled. For example, we determined mainframe equipment is maintained in a secured area and access is limited to authorized personnel. We also reviewed job control procedures to help ensure integrity of all system processing.

We conducted application reviews over State Payroll, Warrant Writer, and SBAS. We interviewed employees of the Department of Administration and the State Auditor's Office to determine policies and procedures. We reviewed input, processing, and output controls for these systems. We also reviewed supporting documentation to determine if controls over data are effective as well as adequate to ensure the accuracy of data during processing phases.

Controls over centralized operations are supplemented by controls established at user agencies. We did not review controls established by agency users.

Compliance

We determined compliance with applicable state laws and rules and Montana Operation Manual policies. Generally, we found the Department of Administration and the State Auditor's Office to be in compliance with applicable laws and state policy.

Chapter II - Information Processing Facility

Information Processing Facility

The Department of Administration, Information Services Division (ISD), manages central data processing services for state government. Central data processing services include, but are not limited to: central mainframe computer processing; design, development, and maintenance support of data processing applications; and disaster recovery facilities for critical data processing applications. Processing is performed on an IBM 3090 computer operating 24 hours a day except for times allocated for system maintenance.

General controls, as defined on page 1, are developed by the computer user to protect assets and limit losses. In our review of ISD's general control environment, we found organizational, procedural, hardware, software, and system development controls existed and were operating as intended. However, we noted weaknesses in physical security and access controls. We discuss these issues in the following sections.

Physical Security and Access Controls

Physical security controls provide security against accidental loss or destruction of data and program files or equipment; and ensure continuous operation of the EDP function. Physical security controls include but are not limited to: safeguard of files, programs and documentation; physical safeguard of the computer facility; and a plan or method to ensure continuity of operations in the event of major destruction of files or hardware breakdown.

Physical access controls ensure access to computer tapes and hardware is limited to authorized personnel. ISD established policies restricting access to ISD work areas. For example, doors to the computer room, tape library, and teleprocessing room are kept locked at all times. Except as discussed below, we determined physical security and access controls were effective.

Mainframe Disaster Recovery Procedures

Disaster recovery procedures provide for continuation of operations following a disaster. User agencies are responsible for recovery of their computer applications following a disaster. ISD is responsible for recovery of the central computer center.

A timely recovery from a major disaster essentially requires a backup facility similar to ISD's computer center. In February 1992, ISD contracted for a backup hotsite with Weyerhauser Corporation in Seattle, Washington, which will provide back-up services for all applications using the mainframe. As of June 1992, ISD had not tested the hotsite or revised its current disaster recovery plan.

In the event of a major disaster, ISD's existing disaster recovery plan would not enable ISD to effectively recover the state mainframe computer to full operating capacity. The current plan provides for backup recovery using a computer operated by the Department of Justice and located at the National Guard Armory. The backup computer does not have sufficient capacity to operate all critical mainframe applications. ISD is developing plans and procedures for hotsite recovery. When tested and fully operational, we believe the hotsite agreement will significantly improve ISD's ability to recover the mainframe computer.

Computer Room Access Policy Should be Documented

Information Services Division uses a mechanical password access system to restrict access to the mainframe computer. The system is activated when a user enters a password through a keypad at the computer room entrance. If the password is valid, the door is opened.

During our review of physical controls, we determined ISD does not have a written policy for changing the computer room password. A Computer Operations Bureau official explained the department has an informal policy to change the password every 90 days or when an employee terminates. However, when we initially questioned the official, he was not aware of the policy and could not explain why the policy was not documented.

Industry standards require computer room access be restricted to authorized individuals. The department should document and communicate its policy for password changes to ensure adequate computer room physical security is maintained. Without written policy and procedures, unauthorized individuals could gain access to the computer room and damage equipment required to run computer programs.

Recommendation #1

We recommend the Department of Administration document and communicate its computer room password policy to department employees.

Computer Room Access by Maintenance Personnel Should be Closely Monitored

Information Services Division contracts with an outside mainframe computer vendor to perform scheduled maintenance and periodic repair to computer hardware. The mainframe computer has built-in system diagnostic equipment to notify ISD and/or the maintenance vendor whenever repair or maintenance is necessary. Maintenance personnel monitor system diagnostics by connecting to the mainframe from an offsite location and notifying ISD officials when they plan to take the system down for repairs.

Maintenance personnel, employed by the computer vendor, access the computer room by entering a password at the computer room entrance. We determined ISD personnel do not supervise maintenance personnel activities. Industry standards suggest whenever maintenance personnel require access, each visit should be authorized by data processing management and recorded in a log. Maintenance personnel should also be accompanied by an operator while in the computer room. Unless access is logged and supervised, maintenance personnel could modify equipment, make unauthorized repairs, or perform unnecessary mainframe computer maintenance.

Information Services Division officials indicated the contract authorizes vendor-employed maintenance personnel access to the computer room whenever repair or maintenance is required. Department officials stated the computer vendor has employed one individual to provide mainframe maintenance to the department. They indicated logging the individual's access during regular working hours is not feasible but agreed to log access and record maintenance activities performed during other work shifts. The officials also agreed to log access full-time and

record activities for all other maintenance personnel. The officials stated ISD personnel are in the computer room when maintenance personnel perform repairs.

Recommendation #2

We recommend the Department of Administration log vendor access to the mainframe computer and record vendor maintenance activities.

Access Control Software

ISD uses an access control software package called Access Control Facility-2 (ACF2) to provide control over electronic access to programs and data stored on the mainframe computer. ACF2 controls access through electronic rules which allow or prevent user access. We reviewed ACF2 rules written for Warrant Writer, State Payroll, and SBAS applications. We identified access control weaknesses which are discussed below and on pages 10 and 16.

Access to Input/Output Library and Agency Programs Should be Restricted

ISD provides input/output (I/O) control services to user agencies. An I/O controller submits agency computer jobs. At the request of mainframe system users, they submit the job for processing; make certain all data files are available; resolve processing problems; follow up on data errors detected during processing; and ensure proper output distribution.

Agency programmers maintain programs and provide ISD a copy of production job control language (JCL). The I/O controller stores multiple agency JCL in the I/O library and executes jobs for agency users on a scheduled or as requested basis.

We determined a user agency's programs are stored in the I/O library. The I/O controller does not need access to programs to submit jobs for agency users. As a result of this access, the I/O controller could make unauthorized changes to agency programs. We discussed this issue with ISD during our FY 1990-91 audit.

As a result, in 1991, ISD requested user agencies to remove programs from the I/O library. A department official believed all programming language had been removed from the I/O library and therefore, had not reviewed the library contents. The department should develop policies and procedures to ensure agency programs are not stored in the I/O library.

We also determined ISD's ACF2 security rule allows two programmers from another agency write access to the I/O library. As a result, the programmers can make unauthorized changes to all agency files stored in the I/O library.

Access to programs and files stored in the I/O library should be limited to authorized persons. We discussed this issue with the department. A department official indicated programmers require access to the I/O library to correct errors and restart programs which process overnight. The department could allow programmers to copy programs from the I/O library to another library instead of allowing changes within the I/O library.

Recommendation #3

We recommend the Department of Administration:

A. Develop policies and procedures to ensure agency programs are not stored in the I/O library.

B. Restrict access to the I/O library to authorized individuals.

Mainframe Passwords Should be Changed Regularly

ACF2 contains a feature which allows ISD's security officer to adjust how often each mainframe user must change their password. ACF2 software has a preset limit of 90 days between password changes. ISD must change the software set limit to use a period other than 90 days as a password limit.

In our Department of Administration financial-compliance audit (91-8) report issued in April 1992, we recommended the department review its mainframe users access rules for compliance

with department accepted standards. The department concurred with our recommendation.

We determined the department adjusted password time limits for the Department of Administration and State Auditor's Office mainframe users to 90 days or less. However, we questioned an ISD official to determine whether ISD has established policies and procedures for all agency user password time limits. The official indicated ISD has informally adopted the 90 day limit as a standard but has given some agency users password time limits greater than 90 days upon request. The official reviews password settings periodically to determine the basis for password time limits greater than 90 days but does not document agency requests or justifications.

Industry standards suggest users change passwords at least every 90 days. Frequent password changes increase data and program security by making unauthorized use more difficult. We determined 265 mainframe users have password time limits greater than 90 days. Unless passwords are changed regularly, unauthorized users could determine a password and access system data and program files. The department should require all mainframe users to change passwords at least every 90 days in accordance with industry standards and department policy. Exceptions to the policy should be documented.

Recommendation #4

We recommend the Department of Administration establish written policies and procedures to ensure all mainframe password time limits are set at 90 days or less.

Chapter III - Department of Administration

Statewide Budget and Accounting System (SBAS)

The Department of Administration, Accounting Bureau, operates the Statewide Budgeting and Accounting System (SBAS). SBAS is an accounting system which provides financial information used to review and control agency financial transactions. The system also provides agency management budgetary control data used for decision making. SBAS provides uniform accounting and reporting for all state agencies by showing receipt, use, and disposition of all public money and property in accordance with generally accepted accounting principles (GAAP).

The Property Accountability and Management System (PAMS) is a subsystem of SBAS. PAMS is used to account for fixed assets owned by state agencies. A detailed description of the PAMS system, and statewide policies for property accounting are contained in Chapter 1700 of the Montana Operations Manual.

Overall, we determined input, processing, and output controls of the SBAS application were effective for fiscal year 1991-92. However, we found areas where controls could be improved to further ensure data security and integrity. This chapter summarizes our review of the Statewide Budgeting and Accounting System.

Programmer Access Should be Restricted

As discussed on page 7, we reviewed access controls over the SBAS application. Accounting Division has established ACF2 rules to limit access to SBAS application programs and datafiles operated on the mainframe computer.

During our review, we determined Department of Administration programmers have unlogged write access to SBAS production programs. Write access allows programmers to access and make changes to SBAS programs. If unlogged, there is no record of programmer access.

Industry standards state programmers do not need access to system or application libraries, which would provide a means of bypassing controls. Their activities should be restricted to test programs and files, with access only to those programs and files

needed for a given assignment. If a programmer is allowed access to production programs or datafiles, the access should be logged and closely monitored.

Access to production programs and datafiles allows programmers to add fictitious payments and change control total balancing programs to disguise differences. The potential exists for unauthorized and untraceable manipulations of critical information. We determined the department logs most but not all programmer access. Unless activity is logged, the security officer reviewing ACF2 reports does not know when programs are accessed and if authorized changes are made.

A department official indicated full-time programmer access is required to maintain SBAS production programs and files and ensure continued SBAS operation. However, we reviewed SBAS ACF2 reports and determined programmer access primarily occurs during month-end. The department has agreed to log all programmer access and develop alternative procedures for programmer access to production programs and datafiles. Alternative procedures may include changes to the library structure or restricting programmer access to production programs and datafiles.

Recommendation #5

We recommend Department of Administration:

A. Log and closely monitor all programmer access to datafiles and production programs.

B. Develop alternative procedures to limit programmer access to production programs and datafiles.

Disaster Recovery Procedures Should Include OE&E

During our three previous annual SBAS audits, we recommended the Department of Administration, Accounting Bureau, incorporate On-line Edit & Entry (OE&E) into its disaster recovery plan. Agencies use OE&E to electronically input and transfer documents to SBAS. During our current review, we again noted the department has not incorporated OE&E into a written disaster recovery plan.

Management should maintain adequate written recovery procedures for critical applications to ensure a rapid system recovery from either short-term interruption or major catastrophe. The Montana Operations Manual (MOMS) section 1-0240.00 outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing the information and resource requirements necessary to maintain the application; and determining alternate procedures which may be necessary if the recovery cannot be completed timely. In addition, all policies and procedures should be thoroughly and adequately documented.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a documented and operable disaster recovery plan agencies may be required to manually prepare documents and the department could not efficiently process the documents to ensure continued functioning of state government.

A department official indicated Information Services Division is responsible for SBAS disaster recovery and the SBAS application will be covered by the Department of Administration hotsite contract. However, ISD is only responsible for mainframe recovery following a disaster. Accounting Bureau should develop OE&E disaster recovery plans which define team member responsibilities, application requirements, alternative procedures, etc.

Recommendation #6

We recommend the Department of Administration develop disaster recovery procedures for the On-line Edit & Entry system in accordance with state policy.

Chapter IV - State Auditor's Office

Introduction

The State Auditor's Office operates the Warrant Writer and State Payroll systems. This chapter summarizes our audit of application controls over these systems and identifies areas where controls should be improved.

Warrant Writer System

The Warrant Writer system controls creation and distribution of most state warrants and the redemption of all state warrants. The system accounts for state warrants issued, outstanding, and redeemed.

The State Auditor's Office and the Department of Administration jointly operate and maintain Warrant Writer. However, the State Auditor's office is primarily responsible for the system. Department of Administration initiates warrant writing and reconciles issued warrants to SBAS. The State Auditor's Office prepares warrants, distributes warrants, and reconciles warrants outstanding to SBAS. Both departments jointly control warrant redemption.

We performed an application review over the Warrant Writer system. We reviewed input, processing, and output controls over Warrant Writer. Overall, we determined controls over Warrant Writer are effective and adequate to ensure accuracy of data during processing phases.

State Payroll System

The State Auditor's Office, State Payroll Department, is responsible for operation, maintenance, and control of the State Payroll system for state government. The State Payroll system processes payroll for all state agencies except six university system units.

Each of the six university units processes its own payroll. Payroll warrants for Montana State University and the University of Montana are printed and distributed at those locations. The four remaining university system units process warrants through SBAS and Warrant Writer but not through State Payroll.

Our review was limited to payroll transactions processed through the State Payroll System. We did not examine controls over payroll processing or distribution at the six university system units.

The State Payroll System is also referred to as the Payroll/Personnel/Position Control system (P/P/P). The payroll component issues and tracks state of Montana employees' wage and benefit payments. The payroll component also calculates payroll deductions, leave and service adjustments, automatic salary increases, and direct bank deposits upon request.

The personnel component records detailed information about each state employee. The personnel database includes information on birth, sex, disability, and emergency notification for each employee. The personnel database also includes information to verify compliance with state and federal labor laws.

The position control component provides management with information necessary for budgeting purposes. The position control component database includes information on employee position number, grade, classification code, date of hire, and longevity. The database also includes information on the amount of money budgeted for specific positions and the portion of budgeted amounts that have been expended for those positions.

State Payroll uses two on-line applications: on-line payroll and on-line forms. Agencies update biweekly prepayroll reports using on-line payroll. Prepayroll reports contain employee payroll data from the previous pay period which agencies update with current pay period information such as regular hours, sick leave hours, vacation, payrates, etc. The on-line forms application allows agencies to enter information for the payroll status, direct deposit, savings bond, leave and service adjustment, and deduction forms. Information input to the on-line applications also updates the personnel and position control applications.

We performed an application review over the State Payroll System. We did not test controls over the position control or personnel components. Controls for these systems are discussed in our performance audit report of the P/P/P System (89P-36) issued February 1990.

We reviewed input, processing, and output controls over the State Payroll System. Overall, we determined input, processing, and output controls were effective for fiscal year 1991-92. However, we found areas where controls could be enhanced to further ensure data security and integrity. This chapter summarizes our review of the State Payroll System.

Programmer and I/O Controller Access Should be Restricted

As discussed on page 7, we reviewed State Payroll access controls. The State Auditor's Office has established ACF2 rules to limit access to payroll application programs and datafiles operating on the state mainframe computer.

During our review, we determined the rules allow Department of Administration programmers unlogged write access to payroll application programs. We also determined Department of Administration input/output (I/O) controllers have unlogged write access to payroll production programs and logged write access to payroll system libraries. Write access allows individuals to make changes to payroll data and programs.

Programmers do not need access to system or application libraries which would provide a means of bypassing controls. Their activities should be restricted to test programs and files with access only to those programs and files needed for a given assignment. They should not be granted access to production programs or files. If a programmer is allowed access to production programs or files, the access should be logged and closely monitored. I/O controller access should also be limited to access necessary to perform job duties.

The programmer or I/O controller could make unauthorized and untraceable changes to programs and/or data. For example, they could add fictitious payments and change control total balancing programs to disguise the difference. Unless activity is logged, the department's security officer reviewing ACF2 reports does not know when programs and datafiles have been accessed and if authorized or unauthorized changes were made.

A department official did not know why programmers or I/O controllers need full-time write access to production programs, datafiles, and system libraries. The official has agreed to log all

programmer access and work with the Department of Administration to develop alternative procedures for programmer access to production programs and datafiles. Alternative procedures may include changes to the library structure or restricting programmer access to production programs and datafiles.

Recommendation #7

We recommend the State Auditor's Office:

A. Log and closely monitor all I/O controller and programmer write access to programs and datafiles.

B. Develop alternative procedures to limit programmer access to production programs and datafiles.

User Control Standards Should Agree to Current Agency Authorization

User control standards establish parameters for individual users as defined by the user's agency. These standards limit or allow changes which users can make to payroll documents. For example, the user control standard may limit one individual to entering specific types of documents and another individual to approving the documents. We identified the following concern with user control standards for on-line payroll and on-line forms applications.

Agencies request user controls by submitting a payroll users worksheet to the State Payroll Department. State Payroll enters the specifications into the payroll database. Only State Payroll Department personnel can inquire, enter, and change control standards.

The department has not established a procedure to match user controls to agency authorization. During our previous audit, we compared user controls to agency worksheets authorizing on-line payroll controls. We determined agency controls submitted to State Payroll were outdated. As a result, three of twenty users had unnecessary access to payroll functions and could improperly enter, approve, or change payroll documents. To

ensure agency submitted controls are current, a procedure to match user controls to agency authorization is necessary.

A department official indicated agencies are responsible for notifying State Payroll when user control changes occur. The department has agreed to send a report of on-line control standards to agencies every six months. The report will require agencies to verify and update changes to employee control standards. However, this does not eliminate the department's responsibility for ensuring the specifications entered on the payroll database are the same as authorized by user agencies.

Recommendation #8

We recommend the State Auditor's Office develop procedures to ensure payroll control standards agree to current agency authorization.

On-Line Forms Input Edits and Error Messages Should be Documented

The on-line forms application contains input edits to assist agency users when entering payroll forms. Input entry edits compare input data to preestablished limits and reasonableness tests. If a user enters invalid data, the edits invoke an error message requesting the user to correct the data.

We requested the State Payroll Department provide us a list of on-line forms input edits and associated error messages. A department official indicated input edits were not documented when the system was developed and, consequently, could not provide us with a complete list of on-line forms input edits.

State Payroll should formally document on-line forms input edits to provide adequate support of edits and edit changes. Documented edit and error definitions provide a basis for making program modifications and facilitate testing procedures. Without adequate documentation, unauthorized edits may be added to the on-line forms application or original edits changed.

We notified the State Payroll Department of our finding. The department has produced a complete list of on-line forms input edits but noted any additional edits or changes are documented on enhancement requests. A complete edit listing with associated error definitions would allow department personnel to easily identify changes or additions to input edits.

Recommendation #9

We recommend the State Auditor's Office formally document on-line form input edits and error definitions.

Procedure Manuals Should be Completed

We reviewed the deputy director and assistant administrator procedure manuals and determined the manuals do not provide complete explanations of duties necessary to process biweekly payroll. Procedure manuals should be prepared which clearly define daily duties and problem resolution procedures.

The deputy director and assistant administrator positions require comprehensive knowledge of the biweekly payroll process. Procedures include but are not limited to: processing agency payroll data through validity edit programs; identifying and correcting errors; verifying completeness of data processed; and preparing payroll reports and warrants.

Currently, the procedure manuals do not provide effective direction to backup personnel for processing biweekly payroll. Complete procedure manuals would provide a source of reference and enable backup or new employees to perform payroll duties properly and process payroll within established time periods.

We notified the department of our finding. A department official indicated the procedure manuals will be updated by June 30, 1993.

Recommendation #10

We recommend the State Auditor's Office prepare complete procedure manuals for the State Payroll Department deputy director and assistant administrator positions.

Revolving Fund Reconciliation Should be Completed Monthly

The State Payroll Department processes state payroll through an Agency Fund revolving account. Employee payroll, taxes, insurance, deductions, and other contributions flow through the account. After payroll processing is completed, the state payroll system automatically updates SBAS by creating a SBAS document which transfers funds from state agencies to the State Auditor's Office. After payroll funds are deposited to this revolving account, State Payroll prepares payroll warrants for distribution. State and federal taxes, insurance, deductions, and other contributions are paid from this account.

State Payroll personnel perform a reconciliation of the account balance recorded on SBAS to payroll records to ensure insurance, state and federal taxes, and voluntary withholdings have been properly deducted and paid. State Payroll procedures require reconciliation of federal and state withholding to SBAS records in order to properly complete quarterly reports.

We determined State Payroll does not reconcile employee voluntary contributions and withholdings to SBAS each month. Employee deductions could be paid to incorrect accounts and remain undetected by State Payroll personnel. The reconciliation should be completed after monthly SBAS transaction reports are completed to ensure accounting or payroll errors are detected and resolved.

We also determined the account has an outstanding cash balance of $7,544 which has remained in the account since 1987. Prior to 1987, the state sent FICA withholdings to the social security administration program within the Public Employees Retirement Division (PERD). Each quarter, PERD forwarded FICA with-

holding to the Federal Social Security Administration office. In 1987 the federal government required FICA withholdings be deposited into an approved depository bank. As a result, the social security program at PERD dissolved. PERD and the Federal Social Security Office did a closeout reconciliation of the final balance owing for FICA and determined the state had an excess of $7,544. PERD transferred the balance to State Payroll. It was deposited into State Payroll's revolving account where it has remained.

Section 17-1-111, MCA, requires the state treasurer to receive all money belonging to the state and not required by law to be received and kept by any other person. Section 17-2-102, MCA, requires all funds deposited in the state treasury be deposited to the General Fund unless statutorily required to be deposited to another fund.

A department official indicated there is no supporting documentation to determine who the funds belong to. Since the source of the funds is unknown and cannot be determined, there are no specific statutory provisions directing the funds to be deposited to a specific fund in the state treasury. State Payroll Department should transfer these funds to the state General Fund.

Recommendation #11

We recommend the State Auditor's Office:

A. Reconcile the SBAS revolving account to payroll records after monthly SBAS reports are completed.

B. Deposit the $7,544 cash balance to the state's General Fund in accordance with state law.

Controls Over Direct Deposit Should be Communicated

We reviewed State Payroll controls over direct deposit and noted a concern regarding the department's reconciliation procedures. State Payroll personnel reconcile direct bank deposit forms to supporting payroll direct deposit registers. This procedure ensures direct deposit funds were properly deposited to payroll recipient bank accounts. If State Payroll does not reconcile the direct bank deposit form to the direct deposit register, payroll distribution errors may not be detected.

We found two of sixteen biweekly direct deposit registers we reviewed did not have the deposit form attached. We could not determine if State Payroll performed the reconciliation. A department official indicated another employee may have performed the two reconciliations during her absence. We determined the department did not have written procedures requiring documentation of the biweekly reconciliation.

We notified the department of our finding. A department official indicated they established written procedures in August 1992 to ensure the direct bank deposit form is properly and promptly reconciled.

Recommendation #12

We recommend the State Auditor's Office continue to reconcile the direct deposit register to the direct bank deposit form and communicate written procedures to department personnel.

Disaster Recovery Procedures Should be Updated

We reviewed the State Payroll Department's disaster recovery plan and determined the department has not updated or tested the plan since fiscal year 1986-87. Since the disaster recovery plan was last updated and tested, the payroll system has undergone significant changes with the addition of on-line payroll and on-line forms applications.

Management should maintain adequate written recovery procedures to ensure a rapid EDP system recovery from either short-term interruption or major catastrophe. The Montana Operations Manual (MOMS) section 1-0240.00 outlines agency responsibilities regarding disaster recovery planning which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain the application; and determining alternate procedures which may be necessary if recovery cannot be completed timely. Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Because the recovery plan is outdated the State Payroll Department may be unable to efficiently recover the payroll application.

The State Auditor's Office is responsible for recovery of the payroll application. A department official indicated disaster recovery procedures for the payroll application will be covered by the hotsite contract entered into by Department of Administration. However, the Department of Administration is only responsible for recovery of the mainframe computer. The State Auditor's Office should define team member assignments, application requirements, alternative procedures, etc., for the on-line payroll and on-line forms applications.

Recommendation #13

We recommend State Auditor's Office develop a payroll application disaster recovery plan in accordance with state policy for the on-line payroll and on-line forms applications.

Payroll Forms Authorization Edit Required

During our review of the on-line forms application, we determined an employee who is authorized to enter and approve payroll forms can both enter and approve the same form. The application does not have an edit which prevents an employee from both entering and approving payroll data.

Effective controls require segregation of functions and responsibilities so no one person has incompatible duties which permit perpetration and concealment of material errors or irregularities. For example, salary changes should be authorized by management. Prior to implementation of on-line forms processing, State Payroll required all payroll forms to be signed by authorized agency personnel. With implementation of the on-line forms application this control was removed.

The ability to enter and approve the same payroll form could allow an employee to make payroll changes for personal gain. We notified the department of our finding. The department modified the on-line payroll forms application in September 1992 to prevent an employee from entering and approving the same form. As a result, we make no recommendation.

Agency Responses

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

STAN STEPHENS, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032

HELENA, MONTANA 59620

November 6, 1992

Mr. Scott A. Seacat
Legislative Auditor
Office of the Legislative Auditor
State Capitol Building
Helena, MT 59620

Dear Mr. Seacat:

We have reviewed the recommendations pertaining to the Central Review Audit of the Information Processing Facility and the Statewide Budget and Accounting System. Our response to each recommendation follows:

Recommendation #1

We recommend the Department of Administration document and communicate its computer room password policy to department employees.

Agency Response:

We concur. We will establish a formal written policy and distribute it to all ISD employees.

Recommendation #2

We recommend the Department of Administration log vendor access to the mainframe computer and record vendor maintenance activities.

Agency Response:

We concur with one limitation: we will log our authorized vendor representative's access to the computer room only during non-prime shift hours (5 p.m. to 8 a.m.). We will implement a policy that vendor personnel other than our authorized vendor representative will not be allowed access to the computer room without prior approval of the shift supervisor or one of his superiors. Such access will be logged. We will establish a written agreement with

the vendor to implement this procedure. We will continue to record major maintenance activities as they take place.

Recommendation #3

We recommend the Department of Administration:

A. Develop policies and procedures to ensure agency programs are not stored in the I/O library.

Agency Response:

We concur. We will review all current and future systems controlled by I/O Control and ensure that source code is not kept in the I/O controllers library.

B. We recommend the Department of Administration restrict access to the I/O library to authorized individuals.

Agency Response:

We concur. We will change this access to "read only" so that maintenance programmers can copy their execution JCL to another library where they can make required changes.

Recommendation #4

We recommend the Department of Administration establish written policies and procedures to ensure all mainframe password time limits are set at 90 days or less.

Agency Response:

We concur. We will establish a formal written policy and distribute it to all Agency Security Officers. The policy will define approved exceptions to the 90 day rule, and ISD will closely monitor these exceptions.

Recommendation #5

We recommend the Department of Administration:

A. Log and closely monitor all programmer access to datafiles and production programs.

B. Develop alternative procedures to limit programmer access to production programs and datafiles.

Agency Response:

We concur. Logging of programmer access to SBAS datafiles has occurred for the past two years. The rules have been changed in the following libraries in order to log programmer access: F01.SBS and F01.PANLIB. The following libraries are used for test or personal reasons and programmer access will not have to be logged or monitored: F01.OEE, F01.SBS.TESTLIB and F01.TSOLIB. The Department will continue to monitor the programmers' access to SBAS datafiles and production libraries. In addition, the Accounting Bureau will work with ISD's Application Services Bureau to develop alternative procedures to limit programmer access to production programs and datafiles.

Recommendation #6

We recommend the Department of Administration develop disaster recovery procedures for the On-line Edit & Entry system in accordance with state policy.

Agency Response:

We concur. By April 1, 1993, the Department will make the changes to its current disaster recovery manual to incorporate disaster recovery procedures for OEE. The Accounting Bureau will work with ISD to develop procedures to manually enter documents through data entry and to incorporate procedures for transferring operations to the computer hotsite.

Thank you for the opportunity to respond to your report recommendations.

Sincerely,

Bob Marks
Director

STATE AUDITOR
STATE OF MONTANA

Andrea "Andy" Bennett
STATE AUDITOR

COMMISSIONER OF INSURANCE
COMMISSIONER OF SECURITIES

November 6, 1992

Rich McRae, EDP Auditor
Legislative Auditor's Office
Capitol Station
Helena, MT 59620

Dear Mr. McRae:

The State Auditor's Office response to the recommendations in the EDP Audit Report for fiscal year 1992, is attached.

With best personal regards, I am

Very truly yours,

Andrea "Andy" Bennett

Andrea "Andy" Bennett
State Auditor

AAB/dwh

Sam W. Mitchell Building/P.O. Box 4009/Helena, Montana 59604/ Telephone: (406) 444-2040/Toll Free 1-800-332-6148

Recommendation # 7

We recommend the State Auditor's Office:

A. Log and closely monitor I/O controller and programmer write access to programs and data files.

B. Develop alternative procedures to limit programmer access to production programs and data files.

We concur.

A. ACF rules have been changed to log I/O controller and programmer write access to production programs and data files.

B. State Payroll will work with ISD in developing procedures to limit programmer access to production programs and data files.

Recommendation # 8

We recommend the State Auditor's Office develop procedures to ensure payroll control standards agree to current agency authorization.

We concur. An enhancement was submitted to ISD to modify the program developed by SBAS to report the current user access. The report has been sent to each agency for their verification. Agency verification has been requested to be returned to State Payroll by November 30, 1992.

Recommendation # 9

We recommend the State Auditor's Office, State Payroll Department, document on-line form edit and error definitions.

We concur. The input edits for the on-line system were not documented separately from the system edits for the edit update program. At the request of the auditor, a complete list of the on-line forms edits was produced. Any additional edits or changes to edits would be documented by an enhancement request, and added to the edit list.

Recommendation # 10

We recommend State Auditor's Office prepare complete procedure manuals for the Deputy Director and Assistant Administrator positions.

We concur. Position manuals will be updated as time permits, with a June 30, 1993, deadline.

Recommendation # 11

We recommend State Auditor's Office:

A. Reconcile the SBAS revolving account to payroll records after monthly SBAS reports are completed.

B. Deposit the $7,544 cash balance to the state's General Fund in accordance with state law.

We concur.

A. Reconciliation has been delayed from time to time due to time constraints, reduction in staff and the fact that our first priority is to produce payroll warrants and direct deposits according to statute. Every effort will be made to ensure reconciliation is up to date.

B. The cash balance of $7,544 has been deposited to the general fund.

Recommendation # 12

We recommend State Auditor's Office continue to reconcile the direct deposit register to the direct bank deposit form and communicate written procedures to department personnel.

We concur. Written procedures have been input into the I/O controllers manual to ensure that the direct bank deposit form is properly and promptly reconciled. The I/O controllers have been briefed as to the correct procedure.

Recommendation # 13

We recommend State Auditor's Office develop a payroll application disaster recovery plan for the on-line payroll and on-line forms applications.

We concur. Requirements for disaster recovery will be developed by June 30, 1993, in conjunction with the hotsite contract with Department of Administration.

AB/dwh